**Blockchain-Technologie: Analyse von “Proof-of-Work” (Bitcoin)**

*Ziad Bougrine*

Abstract

1 – Einleitung

Betrachten wir ein normales System, indem ein Computer oder ein Systemadministrator alles verwalten kann. Dieser kann Pateienteninformationen und Transaktionen in der Datenbank aktualisieren, verwalten, löschen, und hinzufügen.

Oder er sagt einfach, dass Sie ihm 10 000 £ schulden, was gefährlich ist.

Das ist der Hauptgrund, warum Blockchain-Technologie erfunden worden. Aber was ist die Blockchain?

Um die Blockchain zu verstehen, denken Sie an ein Hauptbuch, das öffentliche Transaktionen aufzeichnet. Nehmen wir ein Beispiel, das genauer dieses Konzept erklärt:

Immer wenn Geld von einem Konto auf ein anderes überwiesen wird, wird es für alle sichtbar im Hauptbuch aufgezeichnet, was es den Teilnehmern erschwert, das System zu ändern oder zu betrügen. Wir haben ein bisschen gesehen, was Blockchain ist.

**2 – Einführung in die Blockchain**

**Blockchain Bedeutung**

Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen in einzelnen Blöcken, es ist ein offenes Hauptbuch für Personen, die Datensätze sehen und erstellen können. Jeder Block besteht aus Daten, Hash, vorherigem Hash und Zeitstempel. Entscheidend ist, dass wir spätere Transaktionen auf früheren Transaktionen aufbauen können und diese als richtig bestätigen können, indem wir die Kenntnis der früheren Transaktionen beweisen können. Damit wird es unmöglich gemacht, Existenz oder Inhalt der früheren und späteren Transaktionen zu manipulieren. Andere Teilnehmer der dezentralen Buchführung erkennen eine Manipulation der Blockchain dann an der Inkonsistenz der Blöcke.

Blockchain ist ein Distributed Ledger, diese Technologie nennt sich selbst regieren „Self-governing“, was bedeutet, dass es nicht eine Person gibt, die kontrollieren und machen kann ändern, stattdessen kommen Beiträge von Tausenden von Benutzern, die am Blockchain-Netzwerk teilnehmen, um es funktionsfähig zu machen. Wenn eine Person betrügt, wird sie schnell sein als Betrug angesehen, da der Rest des Netzwerks sie überprüft.

-Konstruktion des Blocks

Ein Block speichert Informationen über Transaktionen, Zeitstempel, vorherigen Hash, Block-Hash.

Ein Block enthält viele Informationen, belegt jedoch nicht viel Speicherplatz. Nehmen wir diese Elemente als Beispiel:

* Magische Zahl : Nummer, die diesen Block als Teil des Netzwerks einer bestimmten Kryptowährung identifiziert.
* Transaktionen : die Hauptinformationen und auch den größten Teil des Blocks
* Transaktionszähler : die Anzahl der im Block gespeicherten Transaktionen
* Block Größe : die maximale Größe der Informationen, die der Block enthält

Was ist die Hauptinformationen, die ein Block (Transaktionen) enthält?

* **Version**: Sie ist benutzbar, um einen neuen Block zu erstellen und um eine neue Version von Software zu identifizieren. Es ist auf 4 Bytes (4 x 8 „bits“) codiert.
* **Vorheriger Block-Hash**: Enthält einen Hash des Headers des vorherigen Blocks (md5, sha256 ...). Es ist auf 32 Bytes (32 x 8 = 256 „bits“) codiert.
* **Hash Merkle root**: Hash of transactions in the [Merkle tree](https://www.investopedia.com/terms/m/merkle-tree.asp) of the current block. Es ist auf 32 Bytes (32 x 8 = 256 „bits“) codiert.
* Es handelt sich um eine Datenstruktur in Form eines Binärbaums, der in Bitcoin und Kryptowährung weit verbreitet ist und zur effizienteren und sichereren Codierung von Daten verwendet wird.
* **Time**: Erstellungszeit des Blocks. Es ist auf 32 Bytes (32 x 8 „bits“) codiert.
* **Bits**: Es ist ein Wert, der die Schwierigkeitsbewertung des Ziel-Hashes und die Schwierigkeit beim Lösen der „Nonce“ angibt. Es ist auf 32 Bytes (32 x 8 „bits“) codiert.
* **Nonce**: Es ist die magische Zahl, die der Miner lösen muss, um einen Block im Blockchain-Netzwerk zu verifizieren und zu schließen.

Achtung:

One 32-bit number in the header is called a nonce—the mining program uses random numbers to "guess" the nonce in the [hash](https://www.investopedia.com/terms/h/hash.asp). When a nonce is verified, the hash is solved when the nonce, or a number less than it, is guessed. Then, the network closes that Block, generates a new one with a header, and the process repeats.

Different mechanisms are used to reach a consensus; the most popular for cryptocurrency is [proof-of-work](https://www.investopedia.com/terms/p/proof-work.asp) (PoW), with proof-of-stake (PoS) becoming more so because of the reduced energy consumption compared to PoW.

- Blockchaining-Mechanismus

Der Blockchain-Mechanismus funktioniert wie eine Linkedlist, er enthält eine Kette von Blöcken

dass jeder Block der Kette aus einem Hash dieses Blocks und einem Hash des vorherigen Blocks zusammengesetzt ist. Es ist derselbe Mechanismus wie bei der Linkedlist, da jeder Knoten der Liste einen Zeiger auf den letzten Knoten enthält.

Was es ermöglicht, über die Kette zu iterieren.

Der erste Block der Kette wird als Genius-Block bezeichnet.

In diesen Situationen sollten wir immer darüber nachdenken, was verdächtige Personen tun könnten, sie könnten die Daten im Block (i) ändern oder manipulieren.

dies führt zu einer Modifikation des tatsächlichen Blocks i und macht den vorherigen Hash im Block (i+1) ungültig. Das bedeutet, dass das Ändern eines Blocks alle nächsten folgenden Blöcke im Blockchain-Netzwerk ungültig macht, was die Qualität der Herstellung einer Kette beweist.

ist dieser Mechanismus gesichert?

Die Verwendung von Hashes reicht nicht aus, um Manipulationen zu verhindern. Computer sind heutzutage sehr schnell und können Tausende von Hashes berechnen. Technisch gesehen können wir einen Block manipulieren und alle nächsten Hashes der nächsten Blöcke neu berechnen, um das Blockchain-Netzwerk wieder gültig zu machen. Aus diesem Grund verwendet Blockchain Proof of Work

in diesen Fällen. Es gibt eine Möglichkeit, dieses Problem zu verhindern. Es ist der berühmte „Proof of Work (POW)“.

Das Grundprinzip von Proof of Work basiert auf der Idee, dass Miner im Netzwerk nachweisen müssen, dass sie einen gewissen Aufwand aufgebracht haben, um einen Block zu erzeugen. Dies stellt mehrere fundamentale Prinzipien von Kryptowährungen wie Bitcoin sicher.

The difficulty (difficulty) of finding a valid hash for the block header is selected in such a way that a new block enters the network about every ten minutes – and with it a certain number of BTC. This ensures the algorithmic money supply growth.

The hash function gives an unpredictable result, that's why we should ask the question "What are the strings input to give to the hash function to produce an exact value?". Because the most property known about the hash function that no one can easily reverse the operation, in other ways miner can't easily reverse the obtained string and get the input of the hash function

That’s why there is concept of mining, the miners are trying to guess the nonce and the order of every parameter that the hash function will take it as a one string and produce a result. There a billiard of operations performed by the miner to reach the value of the input.

Die Schwierigkeit besteht darin, die gewünschte Hash-Ausgabe zu finden. Zum Beispiel Bitcoin, es wird eine Frage gestellt: Wie viele Nullen soll die Ausgabe am Anfang des Strings haben. Je mehr Nullen gefordert sind, desto schwieriger wird es schließlich, den Output zu finden.